

FIG. 1

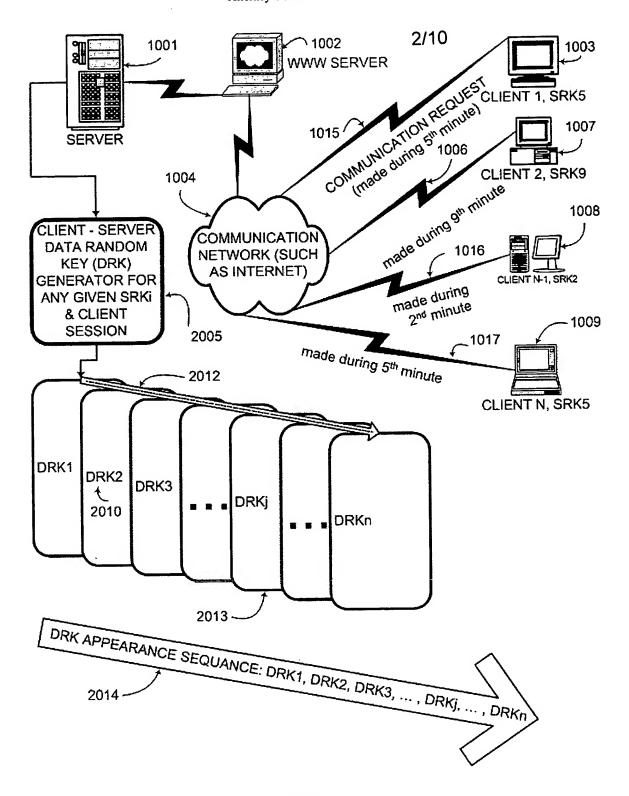
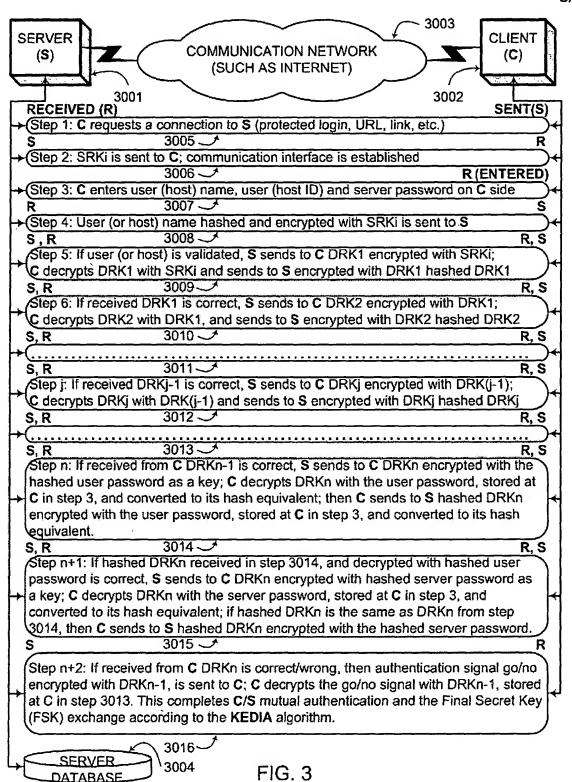


FIG. 2

3/10



4/10

3003 SERVER CLIENT COMMUNICATION NETWORK (C) **(S)** (SUCH AS INTERNET) 3002 3001 SENT(S) RECEIVED(R) Step 6: If received DRK1 is correct, S sends to C DRK2 encrypted with DRK1; C decrypts DRK2 with DRK1, and sends to S encrypted with DRK 2 hashed DRK2 3010 プ 宜 S. R C decrypts DRK2 with DRK1, and Step 6: If received DRK1 is correct, S sends to C DRK2 encrypted with sends to S encryted with DRK2 hashed DRK2 **ORK1** 4002 4001 Conversion array is decrypted with DRK 2 supplied by Server DRK DRK1 (block-cipher encryption/ Generator 2005 (FIG. 2) decryption algorithm) 4003 4004 Client supplies the user password Server supplies the assumed user password to enable bytes, bits, or triggering bytes, or bits, or bytes & bits bytes & bits veiling in DRK2 reassembling in the conversion array <sup>2</sup> 4005 -4006 ByteVU, BitVU, or BBVU is ByteVU, BitVU, or BBVU is applied to veil either bytes, or bits, or bytes & reassembling the coversion array, decrypted before with DRK 1 bits of DRK2 4007 J 4008 DRK 2 is reconstructed to its original form, and C sends to S hashed DRK2, Conversion array, encrypted with treated with either ByteVU, BitVU, or DRK1 (block-cipher encryption BBVU; the final conversion array is algorithm), is sent to client encrypted with DRK 2 4009 <sup>プ</sup> -4010 SERVER DATABASE 3004

FIG. 4

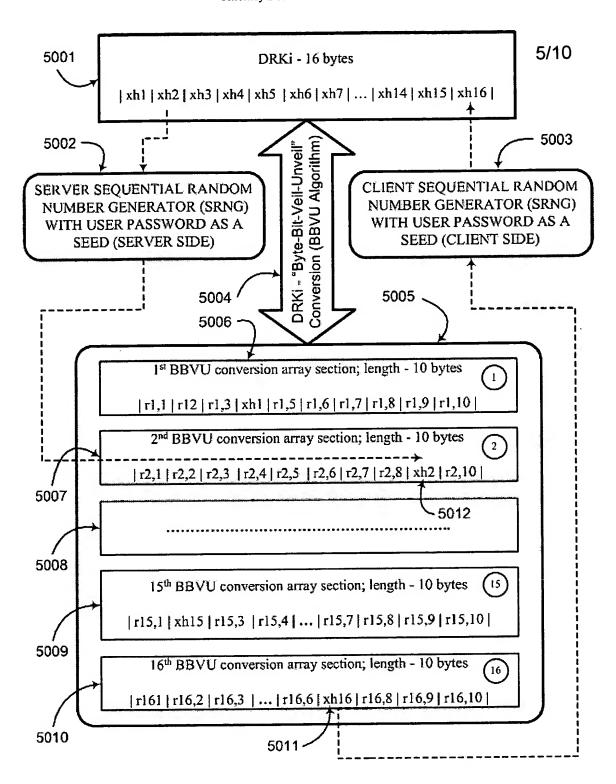


FIG. 5

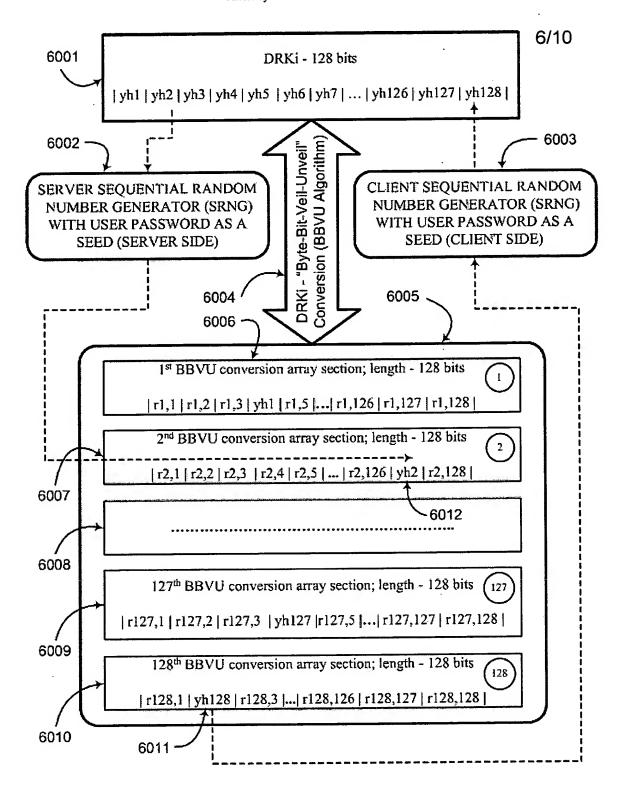


FIG. 6

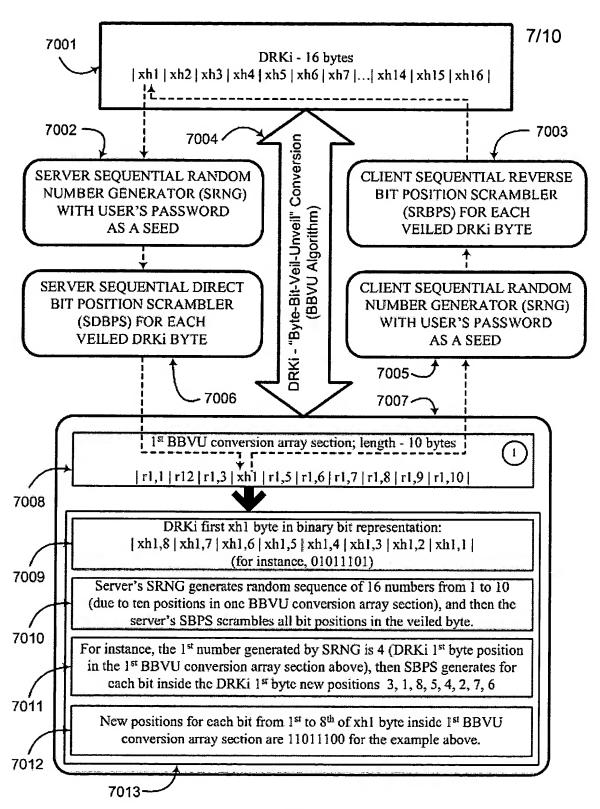


FIG. 7

(Client - Server Architecture; Password Based Mutual Authentication; Part A - SERVER SIDE) MESSAGE ENCRYPT/DECRYPT ITERATIVE AUTHENTICATION (MEDIA) PROTOCOL

8001		8002	8003	8004	8005	9008	8007	8008
SERVER SENT	SENT	1	RECEIVED	E-KEY	D-KEY	ByteVU CA.	SRNG SEED	C-LINE
						SECTIONS,		
						BYTES		
www.s			c connection			OU		to SERVER
			request					
servlets SRK	SRK					ou		to CLIENT
(compiled)	(compiled)							
dB/servlets			h-u-name		SRK	20		to SERVER
dB/servlets DRK1	DRK1			SRK		yes, 16, 25	h-u-password	to CLIENT
dB/servets		_	h-DRK1		DRK1	yes, 16, 25	h-u-password	to SERVER
dB/servlets no	υO	_		SRK		OU		to CLIENT
dB/servlets DRK2	DRK2			DRK1		yes, 16, 25	h-u-password	to CLIENT
dB/servlets			h-DRK2		DRK2	yes, 16, 25	h-u-password	to SERVER
dB/servlets DRK2	DRK2			DRK2		yes, 16, 25	h-s-password	to CLIENT
dB/servlets			h-DRK2		DRK2	yes, 16, 25	h-s-password	to SERVER
dB/servlets go/no	ou/ob			DRK1		yes, 16, 25	h-u-password	to CLIENT

SRK (DRK) - Session (Data) Random Symmetric Encryption Key, ByteVU - "Byte-Veil-Unveil" Algorithm, E - ENCRYPTION, D - DECRYPTION, C - COMMUNICATION, u - user, h - hashed, p - protected c - Client, s - Server, dB - Database, CA - ByteVU Conversion Array Legends: SRNG - Sequential Random Number Generator,

FIG. 8A

8/10

## Inventor: Len L. Mizrah Title: Key Generation Method for Communication Session Encryption and Authentication System Application No.

Attorney Docket No. AIDT 1005-1

	8000	<b>→</b>			-	2		က		4	5	PA 2	9	^	∞	6	10
MESSAGE ENCRYPT/DECRYPT ITERATIVE AUTHENICATION (MEDIA) PROTOCOL (Client - Server Architecture; Password Based Mutual Authentication; Part B - CLIENT SIDE)	8016	CLIENT			WAN/LAN	applet logic		applet GUI		applet logic		applet GUI	applet logic		applet logic		applet GUI
	8015	SENT			p-link / URL			h-u-name			h-DRK1			h-DRK2		h-DRK2	
	8014	RECEIVED				GUI, SRK	(pəliduoo)			DRK1		error message	DRK2		h-DRK2		ou/og
ATIVE AUTHER 3ased Mutual A	8013	ENTERED	BY CLIENT					u-name, s- &	u-passwords								
T ITER/ ssword E	8011 8012	D-KEY E-KEY						SRK			DRK1			DRK2		DRK2	
ECRYP ure; Pas	8011	D-KEY								SRK		SRK	DRK1		DRK2		DRK1
MESSAGE ENCRYPT/D (Client - Server Architect	8010	ByteVU CA,	SECTIONS,	BYTES	no	ou		no		yes, 16, 25	yes, 16, 25	no	yes, 16, 25	yes, 16, 25	yes, 16, 25	yes, 16, 25	yes, 16, 25
MESSAC (Client - 3	6008	SRNG SEED								to CLIENT h-u-password	to SERVER h-u-password		h-u-password	to SERVER h-u-password	h-s-password	h- <b>s</b> -password	h-u-password
	8008	C-LINE			to SERVER	to CLIENT		to SERVER		to CLIENT	to SERVER	to CLIENT	to CLIENT	to SERVER	to CLIENT	to SERVER	to CLIENT

0

SRK (DRK) - Session (Data) Random Symmetric Encryption Key, ByteVÚ - "Byte-Veil-Unveil" Algorithm, E - ENCRYPTION, D - DECRYPTION, C - COMMUNICATION, u - user, h - hashed, p - protected c - Client, s - Server, CA - ByteVU Conversion Array FIG. 8B 8017→ Legends: SRNG - Sequential Random Number Generator,

9/10

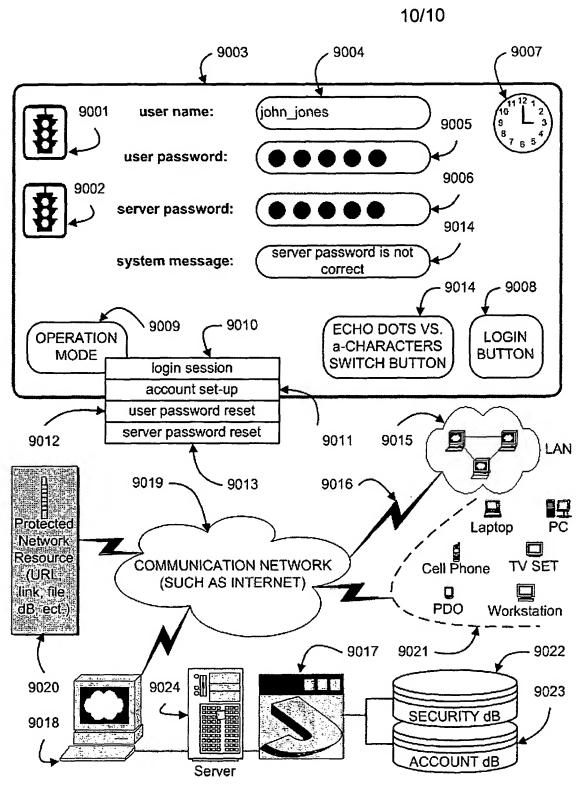


FIG. 9